State of West Virginia
Executive Branch

INFORMATION/CYBER SECURITY

Strategic Plan

Version 5.0

(This page intentionally blank)

TABLE OF CONTENTS

INFORMATION/CYBER SECURITY PROGRAM

Introduction

A significant volume of data is collected from constituents, and stored by West Virginia's Executive Branch agencies. This Information enables government operations, and its ability to provide an array of services.

A documented statewide program for Information/Cyber Security is one element of a comprehensive architecture for the protection of systems and information. The intent of this Strategic Plan is to articulate key elements of the West Virginia Executive Branch security program, and outline the initiatives that support each element. It should be understood that not all controls described are fully implemented, and it is not the intent of this document (for reasons of security) to convey the specific status of each control's implementation.

The West Virginia Office of Technology (WVOT) develops Governor's Executive Branch (GEB) security standards, policies, and procedures for use by Executive organizations, and provides best-practice guidelines for all other State and local public sector organizations. Within these policies as a framework for what needs to be accomplished, while procedures offer detail about how the policies are implemented. Any pre-existing GEB agency policies that address IT or Information/Cyber Security issues, are permitted to be more (but not less) stringent, or restrictive, than those issued by the WV State Chief Technology Officer (CTO). These must be approved by the CTO.

West Virginia must maintain compliance with legal and regulatory requirements. It is essential that the WVOT implement practical measures to protect the State's Information systems (and the associated data) from compromise. Best practices must be followed in order to safeguard **all** forms of Information. It is each agency's responsibility to notify (in writing) the Office of Technology (eSecurity@wv.gov), of any regulatory requirements for which the WVOT must make administrative security accommodation (policy, training, audit), system accommodation (technical controls), or invoke another required control.

The Information/Cyber Security program supports the three essential security requirements of confidentiality, integrity and availability.

An enterprise-wide approach to Information/Cyber Security enables WV State Government's Executive Branch to, in a coordinated and effective progression, reduce risk. Risk can never be eliminated, but it can often be reduced.

The concept of "layered security" involves the use of protective or preventive controls and practices at every opportunity in the information system landscape. Some of the layers in an effective Information/Cyber security program include:

Administrative Controls: Policies, training, audits and enforcement are all obvious administrative controls needed to support a secure organization. The active and visible support of State leadership is an equally important, but less understood factor for the full effectiveness of administrative controls to be realized.
Technical Controls: Multi-factor authentication, best-of-breed firewalls, access control lists (ACL) management, configuration management, whitelisting. Anti-virus, spam filtering, WEB site blocking, encryption, event and flow monitoring, Network Access Control (NAC), Data Loss Prevention (DLP) systems, vulnerability scanning, configuration and patch management, etc.
Physical Security: Standards and compliance, secured doors and secured doorway monitoring for unauthorized persons being allowed in by authorized persons ("tailgating").

The WVOT has utilized the International Standards Organization (*ISO) and* National Institute of Standards and Technolog*y (NIST)* Information/Cyber Security Standards in establishing the West Virginia's Information/Cyber Security architecture.

SECURITY POLICY DEVELOPMENT

Policy is the foundation upon which virtually all successful Information/Cyber security programs are built, and through which the leadership vision for an effective enterprise Information/Cyber security program is communicated to the organization. Policy development is regarded as a collaborative venture, and is enhanced by the input of key stakeholders. The WVOT solicits input from the Governor's Information/Cyber Security Team (GEIST), a group comprised of representatives appointed by Cabinet Secretaries from all GEB department-level organizations, who meet quarterly with each other and the WVOT Security Team.

The WVOT has created a general security policy, as well as other security-related policies and procedures. Agencies may establish more stringent or restrictive IT and security policy, but duplication of content is discouraged. Each agency developing an IT or security policy must submit it to the WVOT for review/approval.

As needed, procedures are developed to specify how operational elements of policy are implemented or executed. While policies are typically published on a public-facing web page, procedures are usually maintained as internal documents, as they sometimes provide operational detail(s) that should not be shared, for security reasons, with the general public.

POLICY INITIATIVES

Initiative 1. Periodically update the existing Executive Branch security policies and procedures

Initiative 2. Create additional policies and procedures as needed

Initiative 3. Review agency information/cyber security policies to ensure consistency, elimination of duplication, and compliance with the Executive Branch security standards

Initiative 4. Maintain copies of all adopted policies online for web (Internet) access

Initiative 5. Develop an effective awareness training strategy for policies, and implement this strategy across the GEB. Involve GEIST stakeholders in policy deployment activities

Initiative 6. Maintain a comprehensive, targeted, set of policies that specifically address the expectations held for employees with critical technical roles, in view of their elevated privileges, requirement for segregation of duties, and the inherent threat potential (e.g. non-malicious accidents) that elevated privileges provide to the holder.

PRIVACY PARTNERSHIP

The Office of Information Security Controls and Compliance (OISC^2) works closely with the West Virginia Privacy Office so that privacy concerns are properly addressed as they relate to technical and administrative security controls. It is essential that privacy and security be viewed as related challenges for the State, and that the policies and standards set forth by these Offices are complementary, and become integrated into all business processes within the Executive Branch. Executive Order 6-06 effectively solidifies the linkage between Information/Cyber Security and Privacy.

PRIVACY SUPPORT INITIATIVES

Initiative 1. Provide security expertise to the Privacy Management Team and State Privacy Officer and staff

Initiative 2. Collaborate with the Chief Privacy Officer on security and privacy concerns, such as incident prevention, preparedness, and response

Initiative 3. Collaborate with the Privacy Office to achieve compliance with privacy mandates, laws, and best practices

RISK MANAGEMENT

In all enterprise environments, there are numerous risks to Information Technology (IT) systems and the data residing within them. Risks can be both internally and externally sourced.

Constantly changing vulnerabilities and threats require risk assessments that are ongoing and thorough, in continuously repeating cycles, identifying new risks, and requiring appropriate risk mitigation actions.

Risk is a relationship between *value, threats, and vulnerabilities*. In the absence of any value, threat, or vulnerability, no risk exists. Value of data tends to increase in most organizations over time (because quantity increases, environmental complexity increases, and investment in data analysis and derivative Information increases). Since the complete elimination of threats and/or vulnerabilities is impossible, risk will always exist, and the increase in value raises the potential loss (dollars at risk) proportionately over time. The reduction of externally-based threats is virtually impossible, although many threats can be blocked, once they are identified. Focus of skills and resources must therefore be directed primarily at the reduction of vulnerabilities, especially around the highest value (potential) targets. Threats must be identified and analyzed, so the weaknesses associated with the targets of these threats – the vulnerabilities – can be reduced, and the threats that ***can*** be blocked, ***are*** blocked.

> **A very real threat is actually any employee that is not consciously compliant with security basics, and fails to adhere to policy and best practices to which (s)he actually has been trained.**
>
> **Put another way, an organization's *failure to resolve identified vulnerabilities, especially "people weakness," presents an opportunity for any threat-agent to exploit.***
>
> **For example: If a parent allows a toddler to cross a busy highway alone, that parent is a threat to the child's well-being, even if the threat-agent that would do the actual harm to the child is the vehicular traffic on the highway.**
>
> **If a user makes a mistake, or intentionally violates policy, this user becomes a threat. This "user-threat" (also called "insider threat") is statistically more likely to cause an incident than external threat-agents, such as malicious-actors and hackers. These internal "user-threats" must be addressed with training, disciplinary action, and elevated cultural expectations.**

Resources available for the reduction of vulnerabilities are limited, so available resources should be prioritized, i.e., allocated first to the vulnerabilities associated with highest value targets. Risk management provides insight into what it is that has the greatest value to the organization, such as the State's most critical systems, and the data that these applications process. The approach we are taking is to classify systems and data in terms of its criticality and its sensitivity (legally protected data such as Protected Health Information (PHI), and Personally Identifiable Information (PII)).

In order to properly manage the broad range of IT risk, the WVOT utilizes a risk life-cycle approach.

- Risk Assessment
- Risk Mitigation
- Evaluation and re-assessment

Risk assessment is the initial phase in the risk management life-cycle. Risk assessment is used to determine each system's criticality to the entity (Department, agency, etc.), sensitivity in content, and to identify potential threats and vulnerabilities for each system. The output of this process identifies appropriate controls for reducing risk during the risk mitigation process. System and data classification is critical to this phase.

The next phase is **risk mitigation**. This involves evaluating, prioritizing, resourcing, and implementing the appropriate, available, and affordable risk-reducing controls/countermeasures to reduce the risks identified during the risk assessment process.

Components of most computer systems are periodically upgraded or replaced, and software applications may be updated with newer versions, or replaced. These hardware and software changes often introduce new vulnerabilities, and previously mitigated risks can return, or new risks can emerge. Thus, the risk management process is ongoing, creating a repeating cycle of **evaluation and re-assessment**, followed by appropriate mitigation.

RISK MANAGEMENT INITIATIVES

Perform for every State computer system identified:

Initiative 1. Review and update documentation of system characterizations: purpose, scope, criticality, sensitivity, platform, age, version, support capability, complexity, etc. (See Data Classification)

Initiative 2. Identify existing relevant threats and vulnerabilities

Initiative 3. Document existing controls in place, or available, to reduce risk

Initiative 4. Determine likelihood and impact of adverse event

Initiative 5. Create a qualitative risk matrix: High, Medium, Low

Initiative 6. Conduct a cost-benefit analysis on prospective risk reduction options

Initiative 7. Select a risk mitigation strategy based upon risk, cost-benefit analysis, and available resources

Initiative 8. Recommend changes in controls/countermeasures. Work toward selection and commitment

Initiative 9. Complete selected mitigation activities. Test effectiveness of mitigation effort

Initiative 10. Create Risk Memoranda to identify residual/acceptable risk after controls/countermeasures

Initiative 11. Monitor system for changes and repeat process at appropriate intervals (go to: Initiative 1)

BUSINESS CONTINUITY PLANS *

Each agency is required to maintain **a Business Continuity and / or a Continuity of Operations** (COOP) plan for identified critical business environments and functions. Each plan must specify how the agency will continue to sustain its critical business functions, and provide services to constituent consumers, until disrupted operations can be fully restored. Continuity plans must be tested and updated by the business units to validate effectiveness of plan, and in collaboration with the Office of Technology, to ensure technical feasibility of plans.

These plans usually identify the core team of individuals who must continue to perform their job functions; identify the physical locations where these individuals will work; identify the office equipment and business tools that these individuals must have at their disposal; and the information systems and data that are vital to their job functions. These plans must include the operational details for supplying the tools and systems needed to the individuals in a time-frame that is depicted in the BC/COOP plan

(*) Note: *The fact that Business Continuity Planning is included in this Strategic planning document* ***does not*** *in any way suggest that this plan creation and maintenance can be accomplished by the WVOT or the OISC*[2].

This topic is included in this document because this planning is a necessary prerequisite to the Disaster Recovery planning and implementation process that is ***offered as a billable service*** *by the IT organization (WVOT, etc.), and cannot be correctly designed without BC/COOP plans that identify critical systems, and prioritizes the order of system recovery.*

Business Continuity planning must be performed by the business units, whose staff must, in addition to address ***prioritization*** *with respect to system restoration.*

INITIATIVES

Initiative 1. Support activity of agency data and system classification, to ensure adequate classification and identification of most critical business systems, in discussions with the Governor's Executive Information Security Team (GEIST – See Security Management Emphasis below in this document)

Initiative 2. Support/validate meaningful alignment between business continuity and disaster recovery plans

Initiative 3. Support/require periodic testing of business continuity plans, in conjunction with the associated disaster recovery plan

DISASTER RECOVERY (DR) PLANS

Disaster recovery plans may be developed with the mistaken thought that they will be useful only in the aftermath of explosions or natural disasters. Sound disaster recovery plans can be just as necessary when a hazard such as airborne asbestos is detected, and causes a business location to become unusable. When an event occurs that disrupts a normal business function, prompt resolution is usually desired and expected, and for most critical functions, this resolution must pre-planned. Disaster recovery addresses the requirement for restoring adequate **IT function(s)** when a significant, or protracted, interruption in service occurs. In some cases, the DR activity may be limited to a redirection of connectivity to an alternate business continuity location, or locations, specified by an affected agency. Often, simply providing Internet access allowing a secure VPN connection to access the State network will suffice. The key, often, is the timeliness of the restored access.

Major disaster recovery activity would be associated with the physical destruction, or functional disruption, of a State data center or critical server or storage location, such as those located at WVOT, DHHR, DEP, TAX, and DoH.

Disaster recovery plans are simply technology services resumption plans. They address emergency equipment acquisition and installation, and/or switching operations to alternate sites where computing equipment has been pre-positioned. The process can include activating additional alternate locations for equipment, including servers, storage, support staff, communications, power, cooling, etc. DR plans require specific instructions for 1) application and data restoration, 2) account login restoration, 3) network and voice communications and other services restoration, 4) expertise deployment, and 5) coordination of efforts to restore most critical services first.

Because there must be an organized and appropriate order of events in the restoration of services, providing the restoration of most critical systems and services first, *DR plan priorities are derived from Business Continuity (BC) or Continuity of Operations (COOP) plans*. This linkage ensures that restoration of a technology function is accomplished according to the pre-determined and documented business need(s).

The recovery of IT functionality to meet the business needs is the responsibility of the WVOT operational units, (as specified in specific agreements with WVOT for this billable service). For this reason, disaster recovery requires a swift, coordinated effort undertaken by staff who may not typically work together under conditions of great urgency. Successful and efficient recovery can best be accomplished when the DR plan has been tested. The WVOT OISC[2] is responsible for supporting and validating the completion, viability, and testing of these disaster recovery plans.

The WVOT Security, Project Management, Client Services, Networking, and Enterprise Applications teams all play key roles in the development of a viable DR plan and, ultimately, the recovery of IT services after a disruptive event.

Coordination (Project Management) between these groups will be essential for the DR planning process, and for the orderly restoration of critical WVOT services, if a disruptive event were to occur.

INITIATIVES

Initiative 1. Where agency agreements exist, verify that disaster recovery plans are completed for each critical business function, and aligned with the associated business continuity plan

Initiative 2. Where agency agreements exist, verify that the plan for adequate periodic testing and validation of disaster recovery plans is completed and documented, along with indicated revisions

SECURITY OPERATIONS CENTER (SOC)

To assist in the reduction of risk, a dynamic view of the network traffic and “events” in the State computing environment, must be maintained. The WVOT Security Operations Center (SOC) utilizes tools that analyze traffic, provide alerts when traffic has known malicious signatures, or anomalous characteristics, and allow technicians to intervene when traffic or events suggest that some violation or malicious activity is taking place in the State network environment. When a problem is suspected, recorded logs can be analyzed to re-construct event history, and the source problem can be identified to a point in time and often to an originating geographic location. The primary system used is referred to as a System Information and Event Management (SIEM) tool. Other tools are used to perform forensic analyses, correlate activities, and identify certain types of criminal activity.

Security Operations Center activities include the monitoring activities, investigations, forensics, WEB monitoring/site blocking, and other system safeguards.

INITIATIVES

Initiative 1. Maintain the full functionality needed in the SOC, including traffic analysis, event correlation and log analysis, threshold alerts, etc.

Initiative 2. Maintain 24x7x365 security surveillance of network traffic and system events for all critical infrastructure components combining threat analysis and alerts to State technicians when any anomalies are detected, correlated, and/or

Initiative 3. Maintain comprehensive WEB activity monitoring and selective site blocking based upon customer requirements

Initiative 4. Develop a state-of-the art situational watch room, combining analyst, management, and executive-level dashboards, giving the agency real-time business security intelligence

Initiative 5. Focus upon the insider threat, and network violation management through the use of effective policy monitoring, reporting and agency enforcement

Initiative 6. Maintain and support the analysis of cyber-security counter-intelligence

TRAINING AND CULTURE

People are generally understood to be the weakest link in securing an enterprise. Even the best technological and physical controls can be defeated easily if the human factor is weak. It is necessary for all State employees be part of the human defense system developed in the State. We ask that all State employees become aware that they are targets, and be mindful that their actions have positive or negative consequences.

The “enlightened” employee can only be achieved with proper awareness training and education that creates an elevated understanding of the tricks, social engineering ploys, “threat vectors” (email attachments and web page links), human vulnerabilities (psychological) that they face, and the personally invoked countermeasures to these non-technical “hacks.” To that end, the WVOT OISC[2] deploys online Information/Cyber Security awareness training. Topics include, but are not limited to, the following:

- Social Engineering – how to avoid being victimized by malicious manipulation techniques
- Password Management – creating, securing, and periodically changing strong, unshared passwords
- Physical Security – supporting controls in place to protect spaces, such as door controls
- Acceptable Use – avoiding unsafe or unethical use of State equipment
- Workplace Security – using precautions to prevent unauthorized access to systems/data
- Internet Security – web use and misuse issues; web filtering and malware challenges
- Incident Reporting responsibility

The operational assumption impressed upon all users is that ***everyone is a target.***

The federal government enacted the *Computer Security Act of 1987* in response to Internet crime and cyber terrorism. This act requires periodic security awareness training for all federal employees who are involved in the management, use, or operation of a computer system. Our State has no less need for Information/Cyber security awareness to be solidified throughout the enterprise.

Making staff aware of threats has proven to be a very cost-effective countermeasure against security violations and/or mishaps. **Gartner analysts Ouellet, Proctor, and Witty (2006) estimated that there is an 0.8 (80%) probability of 25% productivity savings attributable to Information/Cyber Security resulting from the workforce’s elevated awareness of threats, risks, and controls, which reduces the number of security incidents.** Staff trained in a security awareness program will have the knowledge to prevent common incidents and/or to reduce the damage done when an incident does occur.

The expense and human resources involved in creating a set of technological security controls (such as firewalls, anti-virus, encryption, etc.) is essentially undermined in the absence of an informed community of computer users, brought to this status by a comprehensive awareness training program for all State employees (including contractors, and other users of the network).

TRAINING AND CULTURE INITIATIVES

Initiative 1. Provide all Executive Branch employees with security awareness training, annually.

Initiative 2. Establish a process to audit for, and assure, completion of training by all employees, with proper documentation of training history. This must include new employees, contractors, and any other individuals using State computer systems and network

Initiative 3. For the subsets of State employees listed below, establish minimum training standards, and assist with curriculum development that addresses the unique and/or elevated responsibilities and requirement for expertise, commensurate with the role:

- Executive/ Management / Supervisory
- Technician
- Help Desk
- Mobile or Portable Device (smart phone, laptop, usb/thumb drive, portable hard drive) User

Initiative 4. Offer WEB-based Information/Cyber Security awareness training to local governments and other State partners

Initiative 5. Conduct an annual “October is Cyber and Information/Cyber Security Awareness Month” event

- Involve, if possible, the Governor and other State and Federal leaders in reinforcement of the message
- Support the request that the Governor issue a Proclamation, naming October as Cyber and Information/Cyber Security Awareness month
- Publicize the event to the greatest extent possible
- Record the event, if feasible, and make available online, on-demand
- Broadcast the event live, online, if feasible
- Obtain attendee feedback to fuel event improvement in subsequent year(s)

Initiative 6. Periodically introduce new or enhanced training to keep the message “fresh and effecitive.“

INFORMATION/CYBER SECURITY MANAGEMENT EMPHASIS

Under the authority established by Senate Bill 653, effective July 1, 2006, and the Governor's Executive Order 06-06, signed August 16, 2006, and following the mandate of these documents, a high-level Information/Cyber Security Team, known as the Governor's Executive Information Security Team (GEIST) was organized, and has been in place since 2007, to assist with the implementation of Information/Cyber Security initiatives throughout the Governor's Executive Branch of West Virginia State government.

The membership of this team includes the Information Security Administrators (ISA) appointed by the Cabinet Secretaries of each Department or agency. These ISAs provide leadership or oversight in the following areas:

- **Business Continuity planning**
- **Awareness training completion**
- **Risk management initiatives**
- **Data classification initiatives**
- **Communication channel with Departmental leadership, and the Cabinet Secretary**
- **Plan development &testing involvement and oversight**
  - Business continuity and disaster recovery
- **Audits**
  - Facilitate Information Security audits performed by the WVOT OISC[2]
- **Policy implementation**
  - Policy support to the OISC[2], including recommending policy additions, changes, or drafting agency supplements to WVOT-issued policy
  - Policy draft reviews, comments and proposed revisions
  - Monitoring for policy compliance
  - Arranging emphasis or disciplinary action as needed
  - Policy deployment strategy development
- **Policy Enforcement**
  - Appointing Points of Contact (POC) for Network Violation activities
  - Assisting with violation disciplinary recommendations and agency enforcement
- **GEIST team membership and mandatory meeting attendance**
  - ISAs may form teams of support staff for their organizations, and invite them to attend quarterly GEIST meetings, and be added to GEIST Listserv for all notifications.
  - Primary GEIST ISA's from each Department are required to attend quarterly meetings, or furnish the name of a designated substitute to the CISO prior to the meeting.

INITIATIVES

Initiative 1. Maintain an informed and engaged GEIST through quarterly meetings, ad hoc communications, Information/Cyber advisories, and special meetings, as needed

Initiative 2. Elevate the visibility of the Information Security initiatives and the GEIST in organizational units throughout West Virginia State government

Initiative 3. Periodically review the GEIST Charter for relevance and suitability

AUDIT PROGRAM

Under the authority established by Senate Bill 653, effective June 11, 2006, and the Governor's Executive Order 06-06, the WVOT is charged with establishing an audit function to review compliance with all policy provisions that are issued concerning the use of technology, and the security practices governing that use. The WVOT OISC[2] has committed to this audit function with the establishment of an IT Internal Audit Program.

Audit efforts are focused on those areas presenting the highest degree of risk, as well as those areas where risk mitigation will provide the greatest potential benefit to the State. In addition to performing both random and targeted audits in State agencies - examining, evaluating, and reporting on: software applications, related systems, operations, processes, and practices - the Audit Program reviews internal controls within the WVOT operations realm, and conducts audits of selected 3rd party providers, at their off-site locations.

INITIATIVES

Initiative 1. Conduct audits in agencies for compliance with Executive Branch IT policy, including the following:

- User adherence to desktop practices of logging off workstations when leaving unattended, protecting passwords from use by others, and absence of confidential material left in plain view in the desktop area (may be accomplished using the Workplace Assessment initiative)
- Adequate compliance with controls at secured doorways
- Completion of mandatory Information/Cyber Security training
- Annual signoff on reading and agreeing to adhere to the requirements of a State Confidentiality Agreement
- Completion (and testing) of business continuity plan(s)
- Application security

Initiative 2. Conduct audits of technical environments, with emphasis on the WVOT, for compliance with policy and best practices related to the following:

- Segregation of duties
- Strictly followed account management processes
    - Properly authorized requests
    - Priviledge restrictions to minimum necessary for all users and technicians
    - Account termination within guidelines
- Absence of administrative account credentials sharing
    - Use of administrative accounts for administrative duties only
- Current patch levels on system components (servers, workstations)
- Using standardized, hardened, tested configurations (no default configurations in any device)
- Enabling password rule enforcement controls on all systems
- Enabling encyption whereever the encryption option is available
- Disaster Recovery Plan completion and testing.
- Maintaining WEB sites free from publically accessible legally-protected information, and broken links

Initiative 3. Formal reporting of findings to appropriate management with recommendation for corrective action to mitigate identified risk(s)

Initiative 4. Conduct vulnerability scans, and oversee penetration testing as needed to verify system "health."

Initiative 5. Contract for 3rd party auditing services to augment internal audit resources or to perform specialized audit services. Support/facilitate 3rd party audits when engaged to do so.

Initiative 6. Review 3rd party provider agreements and services, including at off-site locations, to ensure adequate security controls. Assure that all 3rd party contracts allow this audit

CERTIFICATION AND ACCREDITATION (C&A)

In the implementation phase of new software applications, or the configuration phase of new hardware (servers, personal computers, wireless access points, etc.) installations, it is vital that the system being moved into production is correctly configured and hardened. Certification is a comprehensive verification and validation of the security of software or hardware, using thorough testing to ensure that security requirements have been met prior to introduction into the production environment. Accreditation is the CTO approval and authorization to introduce any significant technology into the technology environment supported by the WVOT.

The C & A discipline is applied throughout the technology life-cycle to confirm that effective security controls are implemented correctly. While not all technology falls under the C & A discipline, risk analysis should be applied to each technology being considered for deployment, to determine if this control is applicable.

Ultimately, the CTO should authorize, by specific signoff, the introduction of a component, or system (including software systems) of technology into the production environment, based upon its having met the applicable C & A standard(s) for that technology.

INITIATIVES

Initiative 1. Identify responsibility and resources for the development of a C & A program.

Initiative 2. Establish the framework (processes, practices, and procedures) for Certification and Accreditation, collaborating within the Office of Technology, and between the WVOT and its State agency partners.

Initiative 3. Define Certification and Accreditation criteria and scope, meaning: what kinds of technologies must undergo C & A before being moved into production, and what are the standards that must be met for each technology.

Initiative 4. Plan, develop and deliver C & A training to all affected individuals, to unify understanding of the process, and understanding about how to approach product and service rollouts within the C & A framework.

Initiative 5. Map C & A activities to the technology, and project-management life-cycle.

INCIDENT MANAGEMENT AND COMPUTER FORENSICS

Incidents are inevitable, and the variety of incidents experienced range in seriousness from low-impact, to high-impact. With the frequency of reported incidents steadily increasing, the WVOT and OISC^2 must be aggressive in the effort to protect Information and Information systems from disruption, and maintain a readiness to recover from the effects of critical Information/Cyber security incidents. A proven (tested, or previously utilized) incident management plan is recognized as the best preparation for the unexpected event.

The WVOT OISC^2 has policies, standards, and procedures specific to incident response. The OISC^2 has established a central point of contact for reporting incidents (incident@wv.gov), and an automated notification system to contact key responders. The WVOT also offers consulting services and support during the analysis, recovery, and post-mortem phases of incident handling, to any subscribed State organization that is affected by a computer related incident.

Computer forensics capabilities may be required to determine what has occurred (history) in systems, at the workstation level, within a server or network component layer, or on a system-wide level. Forensics tools and skills may be employed to analyze logs, investigate computer abuse, detect and isolate an automated malware infestation or attack, or interrupt and remediate a targeted attack against any system.

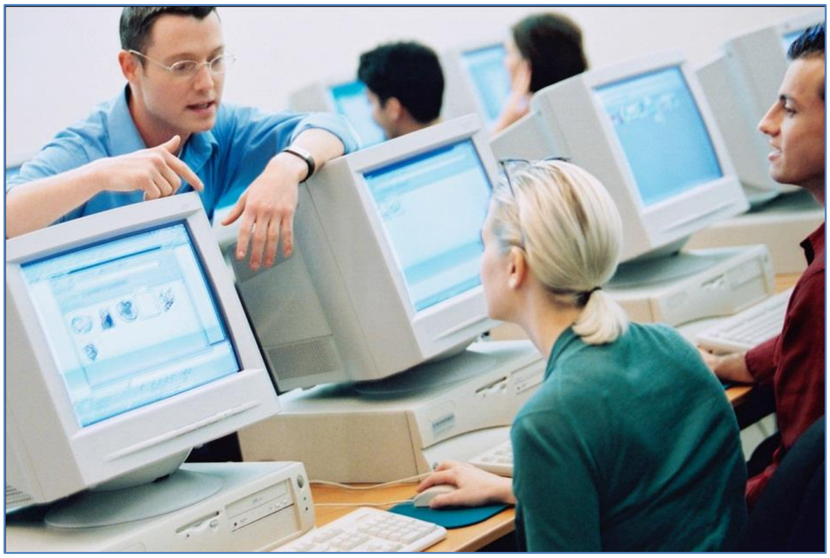
INITIATIVES

Initiative 1. Maintain a Computer Security Incident Response Team (CSIRT)

- Maintain appropriate policies and procedures for notification, response, and recovery from computer security incidents
- Maintain a central point of contact for reporting computer security incidents
- Maintain a service to provide alerts and notification of newly discovered computer vulnerabilities and threats to State, county and local government agencies
- Test the plan on a periodic basis; include testing of all the methods of establishing communications with critical responders

Initiative 2. Maintain adequate forensics skills to accomplish needed investigations professionally, timely, and sutiably documented as needed to provide evidence in a court of law

STAFFING LEVELS AND TEAM DEVELOPMENT



Staffing levels, and building expertise with targeted training, must be adequate to support the mission of the OISC[2]. As this mission grows, and the ongoing requirements of both the technical and administrative components of the OISC[2] grow, capabilities must keep pace. While specialization and depth of skill levels is desirable, Information/Cyber Security staff will be required to assume multiple roles, as they will at times participate in one or more of the following: The audit program, policy development, training development and deployment, system security monitoring, WEB use monitoring and filtering, forensics, incident response, and research and testing functions, to name a few.

Each staff person will ideally be cross-trained, and acquire multiple skill-sets. We will collaborate as a team, and create time-and-task-defined "virtual teams" to complete specific projects, and to meet both short and long-term objectives.

Our team consists of 9 staff, plus the Director, for a total of 10 full-time Information/Cyber Security staff in the OISC[2].

▪ Director	1	FTE
▪ Management:	2	FTE
▪ Technical Security (SOC):	4	FTE
▪ Administrative Security (Audit, Policy, Training, WEB)	3	FTE

Team Development Initiatives:

Initiative 1. Maintain a Job Classification series that closely describes required expertise, and the work, of an Information/Cyber Security professional

Initiative 2. Train and cross-train staff to a multi-disciplinary model as much as possible. Develop staff skills, professionalism, and business awareness. Keep career progression and succession planning in the skills development strategy

FUNDING

The practice of Information/Cyber Security Controls and Compliance in the Executive Branch of West Virginia is a program designed to prevent problems that would be more costly than the expense of instituting the preventative controls themselves. For the most part, the OISC[2] does not generate revenue, however, there are exceptions. For this reason, operational cost must be borne by all agencies in proportion to their use of security services.

Pre-centralization of the Information Security and Compliance function within the WVOT, agencies had varying levels of financial commitment in this area, funded and focused proportionately to the perceived need of agency leadership, and available dollars. There was not an identified correlation between data value (criticality) and investment in safeguards.

Investment in appropriate tools, and maintenance of existing tools, to adequately purchase and staff needed controls, will requires additional funding.

In 2009, a $3/user/month fee was initiated to fund Information/Cyber security. The fee was increased in 2010 to $4/user/month, where it essentially remains in 2014. This fee does not cover the cost of providing adequate Information/Cyber security services to the Executive Branch, and there are important initiatives as yet not undertaken, which shall not be named in this plan for security reasons. Funding at the $6 to $8 level per user per month is a more realistic level.

Funding Initiatives:

Initiative 1. Establish an adequate per seat per user fee for security services that will fund a fully functional Information/Cyber Security Controls and Compliance program as described in this document

INFORMATION/CYBER SECURITY METRICS

In order to measure our work, and to be able to communicate effectively to State leadership, we need to improve a systemization of capturing and reporting metrics. The types of metrics needed vary by the audience for whom they are developed. The audience should ideally have a role in identifying the metrics that are most useful to them.

INITIATIVES

Initiative 1. Work with a representation of partners to develop a set of metrics to be idenified and tracked. Determine the interval, frequency, and format for reporting on these metrics to the various stakeholder groups

Initiative 2. Determine how to derive the metric, and most efficiently capture and report the metric at the specified interval

Initiative 3. Automate the metrics reporting function wherever possible

Initiative 4. Continue to evaluate the effectiveness of the metrics strategy

OUTREACH

Public Sector Partners

The OISC^2 is a leader in providing necessary Information/Cyber Security services in West Virginia's Public Sector. It is therefore essential that we share the resources and capabilities developed within our organization to assist all of the West Virginia governmental entities in any effort they initiate to institute more effective Information/Cyber Security practices. We are committed to supporting public sector partners, including local governments and law enforcement.

Physical Security Partners

Physical Security is the first line of defense, in the practice of Information/Cyber Security. If individuals with malicious intent are able to enter a target facility, their ability to do harm is significantly greater. The use of identification badges, doorway access-controls, surveillance, and other physical controls is basic to effective physical security. Under the current organizational structure in the Executive Branch, physical security is coordinated out of the West Virginia Department of Military Affairs and Public Safety (WV DMAPS). For this reason, it is highly desirable for the WVOT OISC^2 to maintain a strong working relationship with our physical security partners, such as the Division of Protective Services.

Other Security Partners

Important in maintaining an effective Information/Cyber Security program is the exchange of intelligence and expertise among practitioners. The WVOT OISC^2 is actively involved with multiple national organizations, and maintains relationships with other West Virginia State experts including embedded staff within the WV Fusion Center and working contact with the WV Critical Infrastructure Protection Task Force. The WVOT OISC^2 acts as a conduit for Information/Cyber Security alerts and advisories, and as an analytical resource, having participated in the formation of the West Virginia Security Practitioner Workgroup (WVSPWG), a group of security professionals from the Governor's Executive Branch, as well as the Auditor, Secretary of State, Treasurer, Agriculture, National Guard, Fusion Center, and other public sector organizations.

INITIATIVES

Initiative 1. Share expertise, assistance, and training materials with other public sector organizations

Initiative 2. Promote discussions that will enhance the security work of all public sector partners in West Virginia, including organizations such as the WV Department of Military Affairs and Public Safety, the State Treasurer's Office, the Secretary of State, the State Auditor, and other State offices not within the Governor's span of authority, as well as counties and municipalities.

Initiative 3. Maintain active participation with the Multi State – Information Sharing Analysis Center (MS-ISAC), including focus committee participation (currently Training and Awareness, Outreach and Operations), and other groups whose reach is beyond the Governor's Executive Branch

- Continue to update the State alert level on the MS-ISAC portal
- Continue to relay advisories out to partners and constituents as appropriate
- Maintain active involvement in the WVSPWG as described above.

Initiative 4. Maintain active participation in the National Association of State CIOs (NASCIO) Privacy and Security workgroup, and other relevant organizations

Initiative 5. Maintain a working relationship with Legislative Commission on Special Investigations

OFFICE OF TECHNOLOGY PARTNERS

Looking from a security perspective at the State's technical landscape, it is certain that no organization needs greater security self-discipline than the WVOT itself. Our WVOT employees hold the "keys to the kingdom(s)," and have access to virtually every aspect of the computing environment in West Virginia State government. With these elevated access privileges come equally elevated responsibilities, as well as the need for accountability throughout the WVOT technical organization.

It is important that all organizational units in the WVOT work closely together, and particularly closely with the Security team, to ensure that we are creating and using standards in naming conventions, configurations, settings, change control, documentation, and process creation and implementation. All of our initiatives and projects must have security objectives embedded within the architecture and design, and incorporated into the setup configuration and deployment routine for all system components. Information/Cyber Security should be involved as a partner in every design project, and should be an involved participant in regular, technically focused meetings with Client Services, Enterprise Applications, and Networking, and State agencies.

Each organization with a role in the technical setup and administration of system components should align their operational activities with the following **fundamental secuirty concepts**:

- **Least Privilege** – No assignment of privilege to anyone without a need for access
- **Segregation of Duties** – Separation of responsibilities to ensure no conflict of interest, and to ensure accountability
- **Documentation of all critical operational processes, procedures, and security activities** – Diligence is not verifiable without documentation
- **Cross training** to provide redundant skills in critical functional areas – Eliminate skills vulnerabilities created by lack of skills breadth and depth
- **Documentation of all configurations and system setup procedures** - In the event of a failure or "disaster," restoration and recovery operations may need to be completed by someone other than the primary technician assigned to the customary system support function. Thorough documentation reduces dependence on single or specific individuals, especially important during critical situations.
- **Elimination of Single Points of Failure, and Vulnerability to Internal Sabatoge** – Strategies which reduce the chance that critical functions can be adversely impacted by the absence, mistakes, or deliberate actions of a single individual can include rotation of responsibilities and implementation of requirements for multiple individuals to perform and document the processes supporting all aspects of key functions, on a regular basis.

OFFICE OF TECHNOLOGY PARTNERS INITIATIVES

Initiative 1. Review all procurements processed by or through the WVOT having any technical, physical, or administrative security implications, for consistency and compatibility with overall security architecture, designs, technologies, and strategies

Initiative 2. Maintain active participation in all substantive planning sessions within the WVOT and the Executive Branch, or specifically elect to waive participation, documenting the reason(s) for non-participation.

Initiative 3. Monitor all security-related operational activities for compliance with best practices, policies, procedures, and standards, particularly in the six fundamental security concept areas listed above.

Initiative 4. Maintain a comprehensive set of policies, which specifically address the expectations held for employees with critical technical roles in view of their elevated privileges, and the inherent threat potential (e.g. non-malicious accidents) that elevated privileges provide to the holder.

Initiative 5. Develop specialized training for technicians addressing responsibilities and accountability practices, emphasizing the policies and procedures developed solely for their roles, and to assure their compliance with best practices, as privileged-access users within the State's technical infrastructure.

Initiative 6. Promote the development of an Accreditation and Certification Program requiring compliance with all applicable standards including, but not limited to, security standards, documented, with signoff by an authorized authority (CTO or designee) prior to putting any system (hardware or software) into production within the Executive Branch (CTO's span of control). This applies to:
1) Servers,
2) Personal Computers,
3) Portable/mobile devices,
4) Applications,
5) Networking components, phones, and other devices that require setup or customization to work properly in the State environment, with appropriate security settings enabled.

WV INFORMATION/CYBER SECURITY PRINCIPLES

- **Security Awareness** – All employees should understand the elements of their role in the protection of Information systems and the data that these systems contain.

- **Individual Responsibility** – All employees should be responsible for their actions in the use of Information systems, in order to support Information/Cyber Security.

- **Incident Prevention/Reporting** – Employees should strive at all times to prevent security incidents, and report suspected incidents in a timely manner.

- **Ethical Practices** – All employees should adhere to the ethical standards established for public employees in their use of Information systems.

- **Respect** – Employees should recognize the sensitivity of data maintained about citizens, and respect the confidentiality needs and rights of all individuals.

- **Risk Awareness** – As part of the larger risk awareness / risk management process, each employee should review and report any and all risks (threats or vulnerabilities) that may uniquely impact their specific work with Information systems.

- **Culture of Security** – Employees should incorporate secure practices into all of their work activities, handling of Information, and use of Information systems.

- **Security Leadership** – All levels of leadership in West Virginia State government should support sound security practices, and respond constructively and comprehensively to all security initiatives.

- **Process Improvement** - Ongoing and analysis and re-evaluation of risks, threats and vulnerabilities should foster continuous improvements in the security posture, and associated controls.